

Security Standards For Information Technology
July 2006

Policy Area: Information Security Program Charter	Title: Information Technology Security Program Charter for the North Carolina State Chief Information Officer (State CIO) and the Office of Information Technology Services (ITS)
--	--

In North Carolina state government, state laws set out the information technology security requirements and form the Information Security Charter. The matrix below lists those statutes, which define the roles and responsibilities for information technology security, and the compliance procedures that fulfill the legislative mandate.

Section	Statement	Compliance Procedures
147-33.76(b)(1)	<i>The State CIO shall be responsible for developing and administering a comprehensive long-range plan to ensure the proper management of the State's information technology resources. The State CIO shall set technical standards for information technology ... establish information technology security standards.The State CIO is authorized to adopt rules to implement this article</i>	<p>The ITS Information Security Office (ISO), which reports to the State CIO, initiates proposed security policies and standards and reviews those recommended by others.</p> <p>Policies and standards are based on best practices and industry standards including ISO 17799, which has been made available to all executive branch agencies.</p> <p>After review by the ISO, draft security policies and standards are reviewed by the Policy and Legislative Section in the State CIO's Office and the Technology Planning Group, which consists of CIOs from several agencies.</p> <p>The policies and standards also are circulated to the agencies for review and comment, including input from the agency security liaisons.</p> <p>If approved by the State CIO, policies and standards are published on the State CIO's web page. The page also contains the Statewide Information Security Manual and other materials, including a glossary.</p> <p>The ISO operates the Security Portal that provides information technology security alerts and notices to agencies.</p> <p>Agency procedures and practices are</p>
147-33.110	<i>The State Chief Information Officer shall establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including communications and encryption technologies.</i>	

**Security Standards For Information Technology
July 2006**

Section	Statement	Compliance Procedures
		the means through which the statewide standards and policies are implemented.
147-33.110	<i>The State CIO shall review and revise the security standards annually. As part of this function, the State Chief Information Officer shall review periodically existing security standards and practices in place among the various State agencies to determine whether those standards and practices meet statewide security and encryption requirements</i>	Statewide security standards are reviewed at least annually and updated as necessary. The ISO also reviews security standards and practices for other agencies Security standards compliance assessments are conducted and used to evaluate the effectiveness of security standards.
147-33.110	<i>The State Chief Information Officer may assume the direct responsibility of providing for the information technology security of any State agency that fails to adhere to security standards adopted under this Article.</i>	Based upon a review of all available information, including standards, trust levels and incidents, the State CIO recommends improvements to agency information security programs. The State CIO may assume direct responsibility for information technology security where agencies fail to adhere to adopted security standards.
147-33.110	<i>Any actions taken by the State Chief Information Officer under this section shall be reported to the Information Technology Advisory Board at its next scheduled meeting.</i>	The State CIO regularly reports on new security policies, standards, and actions to the Information Technology Advisory Board, which meets at least quarterly.
120-230	<i>There is established the Joint Legislative Oversight Committee on Information Technology.... The Committee shall examine, on a continuing basis, system wide issues affecting State government information technology....</i>	The security policies and standards may be reported to the Joint Legislative Oversight Committee
147-33.112	<i>The State Chief Information Officer shall assess the ability of each agency to comply with the current security enterprise-wide set of standards established pursuant to this section. The assessment shall include, at a minimum, the rate of compliance with the standards in each agency and an assessment of each agency's security organization, network security architecture, and current expenditures for information technology security. The assessment shall also estimate the cost to implement the security measures needed for agencies to fully comply with the standards. Each agency subject to the standards shall submit information required by the State Chief Information Officer for purposes of this assessment. The State Chief Information Officer shall include the information obtained from the assessment in the State Information Technology Plan required under G.S. 147-33.72B.</i>	The State CIO: <ul style="list-style-type: none"> • Provides an assessment tool • Co-ordinates the assessments • Prepares metrics and reports • Includes the information in the biennial State Information Technology Plan.
147-33.113	<i>(a) The head of each State agency shall cooperate with the State Chief Information Officer in the discharge of his or her duties by: (1) Providing the full details of the agency's information</i>	Agencies: <ul style="list-style-type: none"> • Report information technology security incidents to the ISO within 24 hours.

**Security Standards For Information Technology
July 2006**

Section	Statement	Compliance Procedures
	<p><i>technology and operational requirements and of all the agency's information technology security incidents within 24 hours of confirmation.</i></p> <p><i>(2) Providing comprehensive information concerning the information technology security employed to protect the agency's information technology.</i></p> <p><i>(3) Forecasting the parameters of the agency's projected future information technology security needs and capabilities.</i></p> <p><i>(4) Designating an agency liaison in the information technology area to coordinate with the State Chief Information Officer. The liaison shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon its receiving fingerprints from the liaison.</i></p> <p><i>If the liaison has been a resident of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background report shall be provided to the State Chief Information Officer and the head of the agency. In addition, all personnel in the Office of State Auditor who are responsible for information technology security reviews pursuant to G.S. 147-64.6(c)(18) shall be subject to a criminal background report from the State Repository of Criminal Histories, which shall be provided by the State Bureau of Investigation upon receiving fingerprints from the personnel designated by the State Auditor. For designated personnel who have been residents of this State for less than five years, the background report shall include a review of criminal information from both the State and National Repositories of Criminal Histories. The criminal background reports shall be provided to the State Auditor.</i></p> <p><i>(b) The information provided by State agencies to the State Chief Information Officer under this section is protected from public disclosure pursuant to G.S. 132-6.1(c).</i></p>	<ul style="list-style-type: none"> • Upon request, submit information technology security information to the State CIO for review. • Designate agency security liaisons to co-ordinate with the State CIO. • Arrange background checks for agency security liaisons and the results are submitted to the State CIO. • Develop internal processes to comply with statewide security standards and practices and to fulfill all obligations concerning agency reporting to the State CIO. • Develop internal processes, such as non-disclosure agreements to manage their distribution of confidential security information • Provide cost projections of future information technology security needs as part of the expansion budget preparation process. <p>The ISO maintains a database of security liaison information and generates reports as needed.</p> <p>The State CIO, as part of the assessment process, may request that each agency provide evidence of compliance on an annual basis and report the status of agencies' compliance to the Information Technology Advisory Board (ITAB).</p> <p>Requests to ITS for security information concerning an agency are referred to the agency security liaison for proper disposition.</p> <p>Staff in the Office of State Auditor (OSA) responsible for information security reviews must have criminal background checks performed by the SBI. The results of these checks are reported to the State Auditor.</p>

**Security Standards For Information Technology
July 2006**

Section	Statement	Compliance Procedures
G.S. 147-33.89	<p><i>Business continuity planning.</i></p> <p><i>(a) Each State agency shall develop and continually review and update as necessary a business and disaster recovery plan with respect to information technology. Each agency shall establish a disaster recovery planning team to develop the disaster recovery plan and to administer implementation of the plan. In developing the plan, the disaster recovery planning team shall do all of the following:</i></p> <ol style="list-style-type: none"> <i>(1) Consider the organizational, managerial, and technical environments in which the disaster recovery plan must be implemented.</i> <i>(2) Assess the types and likely parameters of disasters most likely to occur and the resultant impacts on the agency's ability to perform its mission.</i> <i>(3) List protective measures to be implemented in anticipation of a natural or man-made disaster.</i> <p><i>(b) Each State agency shall submit its disaster recovery plan on an annual basis to the State Chief Information Officer."</i></p>	<p>State agencies develop and update information technology business continuity plans.</p> <p>Agencies submit disaster recovery plans to the State CIO annually and comply with state policies, standards, and procedures for business continuity planning.</p> <p>The State CIO, through the Strategic Initiatives Office, reviews the plans and reports the review to the individual agencies.</p> <p>The ISO maintains the statewide cyber security incident response plan that supports recovery efforts in the event of an interruption of IT services due to an a cyber attack.</p> <p>Agencies develop cyber incident plans for all critical business systems using the statewide standards, templates and guidelines.</p>
147-33.72B	<p><i>Planning and financing State information technology resources.</i></p> <p><i>(a) In order to provide a systematic process for meeting the State's technology needs, the State Chief Information Officer shall develop a biennial State Information Technology Plan (Plan). The Plan shall be transmitted to the General Assembly by February 1 of each regular session.</i></p> <p><i>(b) The Plan shall include the following elements:</i></p> <ol style="list-style-type: none"> <i>(1) An inventory of current information technology assets and major projects currently in progress. As used in this subdivision, the term 'major project' includes projects subject to review and approval under G.S. 147-33.72C, or that cost more than five hundred thousand dollars (\$500,000) to implement.</i> <i>(2) An evaluation and estimation of the significant unmet needs for information technology resources over a five-year time period. The Plan shall rank the unmet needs in priority order according to their urgency.</i> <i>(3) A statement of the financial requirements posed by the significant unmet needs, together with a recommended funding schedule for each major project currently in progress or recommended for initiation during the upcoming fiscal biennium.</i> <i>(4) An analysis of opportunities for statewide</i> 	<p>Appropriate information about security assets, major security projects and unmet security needs is included in the State CIO's State Information Technology Plan.</p> <p>Agencies are expected to include similar information in their IT plans.</p>

**Security Standards For Information Technology
July 2006**

Section	Statement	Compliance Procedures
	<p><i>initiatives that would yield significant efficiencies or improve effectiveness in State programs.</i></p> <p><i>(c) Each executive agency shall biennially develop an agency information technology plan that includes the information required under subsection (b) of this section. The Office of Information Technology Services shall consult with and assist agencies in the preparation of these plans. Each agency shall submit its plan to the State Chief Information Officer by October 1 of each even-numbered year.</i></p>	
147-33.72C	<p><i>Project approval standards.</i></p> <p><i>(a) Project Review and Approval – The State Chief Information Officer shall:</i></p> <p><i>(1) Review all State agency information technology projects that cost or are expected to cost more than five hundred thousand dollars (\$500,000), whether the project is undertaken in a single phase or component or in multiple phases or components. If the State Chief Information Officer determines a project meets the quality assurance requirements established under this Article, the State Chief Information Officer shall approve the project.</i></p> <p><i>(2) Establish thresholds for determining which information technology projects costing or expected to cost five hundred thousand dollars (\$500,000) or less shall be subject to review and approval under subdivision (a)(1) of this section. When establishing the thresholds, the State Chief Information Officer shall consider factors such as project cost, potential project risk, agency size, and projected budget.</i></p> <p><i>(b) Project Implementation – No State agency shall proceed with an information technology project that is subject to review and approval under subsection (a) of this section until the State CIO approves the project. If a project is not approved, the State CIO shall specify in writing to the agency the grounds for denying the approval. The State CIO shall provide this information to the agency within five business days of the denial.</i></p> <p><i>(c) Suspension of Approval – The State Chief Information Officer may suspend the approval of any information technology project that does not continue to meet the applicable quality assurance standards. This authority extends to any information technology project that costs more than five hundred thousand dollars (\$500,000) to implement regardless of whether the project was originally subject to review and approval under subsection (a) of this section. If the State CIO suspends approval of a project, the State CIO shall specify in writing to the agency the grounds</i></p>	<p>The ISO participates in the project review process and reviews each project for information security requirements.</p> <p>As part of the project management process the agency is asked to provide:</p> <ul style="list-style-type: none"> • A security contact. • A summary of the function of the application and the community of users. • A classification of data for legal requirements, such as HIPAA, IRS rules, and state confidentiality statutes. • A risk assessment. • The security architecture. <p>The State Chief Information Security Officer (CISO) reviews and advises on the adequacy of the planned information security measures included in the project plan.</p> <p>As the project moves through its various phases, the State CISO continues reviewing the project progress to make certain that appropriate security controls are in place and that the application design complies with the statewide information security standards.</p>

Security Standards For Information Technology
July 2006

Section	Statement	Compliance Procedures
	<p><i>for suspending the approval. The State CIO shall provide this information to the agency within five business days of the suspension.</i></p> <p><i>The Office of Information Technology Services shall report any suspension immediately to the Office of the State Controller and the Office of State Budget and Management. The Office of State Budget and Management shall not allow any additional expenditure of funds for a project that is no longer approved by the State Chief Information Officer.</i></p> <p><i>(d) General Quality Assurance- Information technology projects that are not subject to review and approval under subsection (a) of this section shall meet all other standards established under this Article.</i></p> <p><i>(e) Performance Contracting. – All contracts between a State agency and a private party for information technology projects shall include provisions for vendor performance review and accountability. The State CIO may require that these contract provisions include monetary penalties for projects that are not completed within the specified time period or that involve costs in excess of those specified in the contract. The State CIO may require contract provisions requiring a vendor to provide a performance bond.</i></p>	
147-33.72E	<p><i>Project Management Standards</i></p> <p><i>(a) Agency Responsibilities. – Each agency shall provide for a project manager who meets the applicable quality assurance standards for each information technology project that is subject to approval under G.S. 143-33.72C(a). The project manager shall be subject to the review and approval of the State Chief Information Officer.</i></p> <p><i>The agency project manager shall provide periodic reports to the project management assistant assigned to the project by the State CIO under subsection (b) of this section. The reports shall include information regarding project costs, issues related to hardware, software, or training, projected and actual completion dates, and any other information related to the implementation of the information technology project.</i></p> <p><i>(b) State Chief Information Officer Responsibilities. – The State Chief Information Officer shall designate a project management assistant from the Office of Information Technology Services for projects that receive approval under G.S. 147-33.72C(a). The State Chief Information Officer may designate a project management assistant for any other information technology project.</i></p> <p><i>The project management assistant shall advise the agency with the initial planning of a project, the content and design of any request for proposals, contract development, procurement, and architectural and other technical reviews. The project management assistant shall also monitor agency progress in the development and implementation of the project and shall provide status reports to the State Chief Information Officer, including recommendations regarding continued approval of the project.</i></p>	<p>The ISO staff works with the project manager assigned by the State CIO to address the security issues as they arise.</p>

**Security Standards For Information Technology
July 2006**

Section	Statement	Compliance Procedures
147-33.72G	<p><i>Information Technology Board.</i></p> <p><i>(a) Creation; Membership. – The Information Technology Advisory Board is established and shall be located within the Office of Information Technology Services for organizational, budgetary, and administrative purposes. The Board shall consist of 12 members, four appointed by the President Pro Tempore of the Senate, and four appointed by the Speaker of the House of Representatives. All appointments shall be from among persons knowledgeable in the subject area and having experience with State government or information technology deployment within large organizations. Each member shall serve at the pleasure of the officer who appointed the member. The Governor shall designate a chair from among the membership.</i></p> <p><i>(b) Conflicts of Interest. - Members of the Advisory Board shall not serve on the board of directors or other governing body of, be employed by, or receive any remuneration of any kind from any information systems, computer hardware, computer software, or telecommunications vendor of goods and services to the State of North Carolina. No member of the Advisory Board shall vote on an action affecting solely that person's State agency.</i></p> <p><i>(c) Powers and Duties. - The Board shall:</i></p> <p><i>(1) Review and comment on the State Information Technology Plan developed by the State Chief Information Officer under G.S. 147-33.72B(b).</i></p> <p><i>(2) Review and comment on the information technology plans of the executive agencies prepared under G.S. 147-33.72B(c).</i></p> <p><i>(3) Review and comment on the statewide technology initiatives developed by the State Chief Information Officer.</i></p> <p><i>(d) Meetings. - The Information Technology Advisory Board shall adopt bylaws containing rules governing its meeting procedures. The Board shall meet at least quarterly. The Office of Information Technology Services shall provide administrative staff and facilities for Advisory Board meetings.</i></p> <p><i>The expenses of the Board shall be paid from receipts available to the Office of Information Technology Services as requested by the Board. Advisory Board members shall receive per diem, subsistence, and travel allowances as follows:</i></p> <p><i>(1) Commission members who are officials or employees of the State or of local government agencies, at the rate established in G.S. 138-6;</i></p> <p><i>and</i></p> <p><i>(2) All other commission members, at the rate established in G.S. 138-5.</i></p>	<p>The State CISO and ISO staff provide reports to the ITAB on information security and privacy issues, as required by law.</p> <p>The State CISO and ISO staff evaluate any comments made by the board on security initiatives.</p>
G.S. 147-64.6(c)	<p><i>The Auditor shall, after consultation and in coordination with the State Chief Information Officer, assess, confirm, and report on the security practices of information</i></p>	<p>ITS consults with the State Auditor and assists with the coordination of security audits performed by the</p>

**Security Standards For Information Technology
July 2006**

Section	Statement	Compliance Procedures
	<p><i>technology systems. If an agency has adopted standards pursuant to G.S. 147-33.111(a) or (2), the audit shall be in accordance with those standards. The Auditor's assessment of information security practices shall include an assessment of network vulnerability. The Auditor may conduct network penetration or any similar procedure as the Auditor may deem necessary. The Auditor may enter into a contract with a State agency under G.S. 147-33.111(c) for an assessment of network vulnerability, including network penetration or any similar procedure. Any contract with the Auditor for the assessment and testing shall be on a cost-reimbursement basis. The Auditor may investigate reported information technology security breaches, cyber attacks, and cyber fraud in State government. The Auditor shall issue public reports on the general results of the reviews undertaken pursuant to this subdivision but may provide agencies with detailed reports of the security issues identified pursuant to this subdivision which shall not be disclosed as provided in G.S. 132-6.1(c). The Auditor shall provide the State Chief Information Officer with detailed reports of the security issues identified pursuant to this subdivision. For the purposes of this subdivision only, the Auditor is exempt from the provisions of Article 3 of Chapter 143 of the General Statutes in retaining contractors.</i></p>	<p>Auditor.</p> <p>ITS shares information with the State Auditor about compliance with security standards.</p> <p>The OSA provides the State CIO with detailed reports of security issues identified.</p> <p>The State CIO may use results of vulnerability assessments to evaluate security standards effectiveness and compliance.</p> <p>The OSA audits for agency compliance with security standards and practices.</p> <p>A memorandum of understanding exists between ITS, OSA, SBI and the Attorney General's Office setting standard practice for security incidents on the state's network.</p>